

# PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-215294

(43)Date of publication of application : 04.08.2000

---

(51)Int.Cl.

G06K 19/10

G06T 7/00

---

(21)Application number : 11-016944

(71)Applicant : OKI ELECTRIC IND CO LTD

(22)Date of filing : 26.01.1999

(72)Inventor : SUZUKI HIROSHI

ARAI KAZUAKI

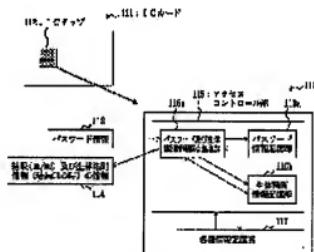
---

## (54) IC CARD INCORPORATING LIVING BODY IDENTIFICATION INFORMATION AND IDENTITY CERTIFICATION METHOD

### (57)Abstract:

**PROBLEM TO BE SOLVED:** To provide an IC card incorporating living body identification information improvable in reliability by strictly certifying identity and its identity certification method.

**SOLUTION:** The IC card incorporating living body identification information is provided with a living body identification information storage part 116b stored in the IC card 111 and a living body identification information collation processing part 115a collating living body identification information stored in the living body identification information storage part 116b with living body identification information which a camera reads.



---

## LEGAL STATUS

[Date of request for examination] 13.12.2005

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's  
decision of rejection]

[Date of requesting appeal against  
examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁 (JP)

(12) 公開特許公報 (A)

(11)特許出願番号

特開2000-215294

(P2000-215294A)

(43)公開日 平成12年8月4日 (2000.8.4)

(51)Int.Cl.<sup>7</sup>

G 0 6 K 19/10  
G 0 6 T 7/00

識別記号

F I

G 0 6 K 19/00  
G 0 6 F 15/62

マーク<sup>7</sup> (参考)

S 5 B 0 3 5  
4 6 5 K 5 B 0 4 3

審査請求 未請求 請求項の数 6 O.L. (全 10 頁)

(21)出願番号 特願平11-16944

(71)出願人 000000295

(22)出願日 平成11年1月26日 (1999.1.26)

沖電気工業株式会社

東京都港区虎ノ門1丁目7番12号

(72)発明者 鈴木 博

東京都港区虎ノ門1丁目7番12号 沖電気  
工業株式会社内

(72)発明者 新井 一明

東京都港区虎ノ門1丁目7番12号 沖電気  
工業株式会社内

(74)代理人 100089635

弁理士 清水 守 (外1名)

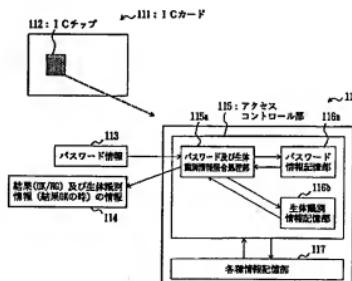
最終頁に続く

(54)【発明の名称】 生体識別情報内蔵型ICカード及びその本人認証方法

(57)【要約】

【課題】 本人認証を厳格にすることにより、信頼性の向上を図り得る生体識別情報内蔵型ICカード及びその本人認証方法を提供する。

【解決手段】 生体識別情報内蔵型ICカードであつて、ICカード111内に格納される生体識別情報記憶部116bと、この生体識別情報記憶部116bに記憶された生体識別情報とカメラから読み取られた生体識別情報をとを照合する生体識別情報照合処理部115aとを具備するようにしたものである。



## 【特許請求の範囲】

【請求項1】 生体識別情報内蔵型ICカードであって、(a) ICカード内に格納される生体識別情報記憶部と、(b) 該生体識別情報記憶部に記憶された生体識別情報とを照合する生体識別照合処理部とを備備することを特徴とする生体識別情報内蔵型ICカード。

【請求項2】 請求項1記載の生体識別情報内蔵型ICカードであって、前記ICカード内に格納されるパスワード情報を記憶するパスワード情報記憶部と、該パスワード情報記憶部に記憶されたパスワード情報と入力装置から入力されるパスワード情報を照合するパスワード情報照合処理部とを備備することを特徴とする生体識別情報内蔵型ICカード。

【請求項3】 請求項1記載の生体識別情報内蔵型ICカードであって、前記生体識別情報はアイリスピターン情報をすることを特徴とする生体識別情報内蔵型ICカード。

【請求項4】 ICカードを用いた本人認証方法において、(a) ICカード内に生体識別情報を内蔵し、

(b) 該生体識別情報と本人固有の生体識別情報をICカード内の生体識別照合処理部で処理し、本人認証を行なうことを特徴とするICカードを用いた本人認証方法。

【請求項5】 請求項4記載のICカードを用いた本人認証方法において、前記ICカード内に照合履歴を記憶させ、該ICカード内の照合履歴を逐次更新していくことを特徴とするICカードを用いた本人認証方法。

【請求項6】 請求項4記載のICカードを用いた本人認証方法において、前記生体識別情報はアイリスピターン情報をすることを特徴とするICカードを用いた本人認証方法。

## 【発明の詳細な説明】

## 【0001】

【発明の属する技術分野】本発明は、生体識別情報内蔵型ICカード及びその本人認証方法に関するものである。

## 【0002】

【従来の技術】従来のICカードを利用した本人(個人)認証方法は本人の記憶するパスワードによるものであった。

【0003】図13はかかる従来のICカードを利用した本人認証手段の模式図である。

【0004】この図において、11はICカード、12はそのICカード内に内蔵されるICチップ、13はパスワード情報、14はパスワード(本人認証)の結果情報、15はICチップ内のアクセスコントロール部、16はそのアクセスコントロール部のパスワード照合処理部、17はパスワード情報記憶部、18は各種情報記憶部である。

10

【0005】この図に示すように、パスワード情報13と、その結果(OK/NG)情報14はICカード11と外部装置との間でやりとりされるように構成されている。

【0006】図14は従来型の入退室管理システムにおける本人認証手段の模式図である。

【0007】この図に示すように、入退室する部屋のドア29の前に人が立っており、その人のアイリスピターン20のアイリスピターン26を読み取るためにカメラ21が設置されている。また、ドアの横にはIDカード読み取り装置(ICカードリーダー)23が設置されている。さらに、それらの機器を制御する入退室管理システム25が背後にあり、その中にはアイリスピターン26、利用者ID等を登録したデータベース24が存在する。なお、22はICカードである。

【0008】ここで、アイリスとは、生体識別情報の一つで、人の目の虹彩部分を表している。アイリスピターンとは、その虹彩パターンを符号化したデジタル情報である。

## 【0009】

【発明が解決しようとする課題】しかしながら、以上述べた本人認証方法においては、ICカードの機能面で、いかにもセキュリティ機能が優れたものであっても、ICカードとパスワードの盗難といったケースで不正使用される場合があった。

【0010】具体的には、ICカードとパスワードの盗難により、(1) ICカード内の個人情報などの情報の取り出し(プライバシーの漏洩)、(2) 他人になりますことによる口座からの金銭不正引き出し、入出管理されている室内への不正入場、セキュリティ管理されてる金庫からの不正持ち出しなどが可能であった。

【0011】また、従来の場合は、本人確認データが本人が所持するカードに内蔵されるのではなく、集中的にデータを記憶するデータ記憶装置に保持するようにしているため、そのデータが盗まれて不正なカードの偽造や不正使用(アイリスの偽装)などの問題が内在している。

【0012】本発明は、上記問題点を解決するために、本人認証を厳格にすることにより、信頼性の向上を図り得る生体識別情報内蔵型ICカード及びその本人認証方法を提供することを目的とする。

## 【0013】

【課題を解決するための手段】本発明は、上記目的を達成するために、

(1) 生体識別情報内蔵型ICカードであって、ICカード内に格納される生体識別情報記憶部と、この生体識別情報記憶部に記憶された生体識別情報と撮像装置から読み取られた生体識別情報を照合する生体識別照合処理部とを備備するようにしたものである。

【0014】(2) 上記(1)記載の生体識別情報内蔵

40

50

型ICカードであって、前記ICカード内に格納されるパスワード情報を記憶するパスワード情報記憶部と、このパスワード情報記憶部に記憶されたパスワード情報と入力装置から入力されるパスワード情報を照合するパスワード情報照合処理部とを具備するようにしたものである。

【0015】(3) 上記(1)記載の生体識別情報内蔵型ICカードであって、前記生体識別情報はアイリスパターン情報であることを特徴とする。

【0016】(4) ICカードを用いた本人認証方法において、ICカード内に生体識別情報を内蔵し、この生体識別情報と本人固有の生体識別情報をICカード内の生体識別照合処理部で処理し、本人認証を行うようにしたものである。

【0017】(5) 上記(4)記載のICカードを用いた本人認証方法において、前記ICカード内に照合履歴を記憶させ、このICカード内の照合履歴を逐次更新していくようにしたるものである。

【0018】(6) 上記(4)記載のICカードを用いた本人認証方法において、前記生体識別情報はアイリスパターン情報であることを特徴とする。

【0019】

【発明の実施の形態】以下、本発明の実施の形態について詳細に説明する。

【0020】まず、本発明の第1実施例について説明する。

【0021】図1は本発明の第1実施例を示すICカードを利用した本人認証手段の模式図である。

【0022】この図において、111はICカード、112はそのICカード内に記憶されるICチップ、113はパスワード情報、114はパスワード情報及び生体識別情報(本人認証)の結果の情報、115はICチップ内のアクセスコントロール部、115aはそのアクセスコントロール部のパスワード及び生体識別情報照合処理部、116aはパスワード情報記憶部、116bは生体識別情報(ここでは、アイリスパターン)記憶部、117は各種情報記憶部である。

【0023】このように、ICチップ112内には、アクセスコントロール部115、(パスワード情報及び生体識別情報照合処理部115a、パスワード情報記憶部1

116a、アイリスパターンなどの生体識別情報記憶部116b)、その他個人情報を記録してある各種情報記憶部117から構成されており、ICカード保持者のパスワード情報113の入力と、その照合結果情報(パスワード(O/K/NG)及び生体識別情報(結果OKの時)114の出力は、ICカード111と外部装置との間でやりとりされるように構成されている。

【0024】図2は、図1に示した生体識別情報内蔵ICカードによる本人認証を、入退室管理システムに応用した例を説明するための模式図である。

【0025】入退室する部屋のドア122の前に人が立っており、その人のアイリス120のアイリスピターン126を読み取るためのアイリスピターン認識用カメラ121がドア122の近傍に設置されている。また、ドア122の横には暗証入力装置123とICカード読み取り装置(ICカードリーダ)124が設置されている。さらに、それらの機器を制御する入退室管理システム125が背後にあり、その中には利用者ID等を登録したデータベース129が存在する。

【0026】ICカード111内には、ICカード所有者の生体識別情報であるアイリスピターン情報Aが内蔵されており、パスワード情報照合がOKならアイリスピターン情報と利用者IDを読み取れるようになっている。

【0027】以下、この実施例の本人認証の方法について図3を参照しながら説明する。

【0028】(1)まず、入退室管理システム125側では、入室しようとしている人がドア122の前に立ちICカード111をICカード読み取り装置(ICカードリーダ)124に入力すると、アイリスピターン認識用カメラ121は立っている人のアイリスピターン情報を読み込む(ステップS1)。

【0029】(2)次いで、暗証入力装置123からパスワード情報113を入力し、そのパスワード情報113を元にICカード111のアイリスピターン情報Aを要求する(ステップS2)。

【0030】(3)また、ICカード111側では、外部の装置からパスワード情報113を受け取り(ステップS11)、ICカード111内のパスワード情報113と比較照合し(ステップS12)、パスワード情報113の照合結果がOKの場合には、そのICカード111に登録されているアイリスピターン情報Aと利用者のアイリスピターン情報を利用者IDを読み取り(ステップS13)、パスワード照合結果及びそのICカード111に登録されている各種情報(アイリスピターン、利用者ID)を回答する(ステップS14)。

【0031】(4)また、入退室管理システム125側では、カメラ121から読み込んだアイリスピターン126とICカード111内のアイリスピターンとを比較照合する(ステップS3)。

【0032】(5)次に、照合結果を判定する(ステップS4)。

【0033】(6)次に、ステップS4において結果がOKであれば、パスワード情報113を検索する(ステップS5)。

【0034】(7)次に、パスワード情報113をチェックする(ステップS6)。

【0035】(8)次に、パスワード情報113がOKであれば、ドアを開く(ステップS7)。

【0036】上記したように、本発明の第1実施例によ

れば、

(A) 入退室管理システム側のデータベースに利用者のアイリストバーン情報を登録しておく必要がないため、アイリストバーン情報の漏洩・改ざんされることがなくなる。

【0037】(B) 利用者は自分のアイリストバーン情報を登録されているICカードを自分自身で持ち歩けることから安心して利用することができる。

【0038】(C) ICカードを紛失した場合でも、ICカード内のアイリストバーン情報を書き換えられないため、他人が自分になりますてそのICカードを利用して入室する心配がない。

【0039】(D) アイリストバーンはICカード内に格納されており、オンライン化でやり取りする必要がないため、広域に点在するドアなど、オンライン化が困難な場合であっても、各所にアイリストバーンデータのデータベースを置く必要がなく対応可能である。コスト面・保守面でも有利である。

【0040】(E) パスワードによる照合、アイリズによる照合、パスワード+アイリズによる2重の照合など、照合の方法はICカードを利用するシステムによって自由に決められるため、入退室のセキュリティレベル(セキュリティが必要度)に応じて選択可能である。しかし、パスワードが盗まれればICカード内の各種情報が読まれてしまう危険はある。(注:パスワード自体はICカードから読み取れない仕組みであり、続けて3回パスワードを間違えるとICカード自身がカードを無効化するなどの仕組みはついている。)

(F) オンライン化の必要性がないため、ICカードは異なるシステム間で共通に利用しやすい。

【0041】等の効果がある。

【0042】次に、本発明の第2実施例について説明する。

【0043】図4は本発明の第2実施例を示すICカードを利用した本人認証の模式図である。

【0044】この図において、211はICカードであり、その内部にはICチップ212が埋め込まれている。ICチップ212内は、アクセスコントロール部215(パスワード照合処理部215a、パスワード情報記憶部216a、生体識別照合処理部215b、アイリストバーンなどの生体識別情報記憶部216b)、その他個人情報を記録してある各種情報記憶部218から構成される。ICカード保持者による生体識別情報(+パスワード)213の入力と結果(照合率)情報214の出力は、ICカード211と外部装置との間でやりとりされるデータの種類を表している。

【0045】図5は、図4に示した生体識別内蔵ICカードによる本人認証方法を、入退室管理システムに応用了した例を説明するための模式図である。

【0046】図5に示すように、入退室する部屋のドア

10

222の前に人が立っており、その人のアイリストバーン情報220を読み取るためアイリストバーン認識用カメラ221(撮像装置)が設置されている。また、ドア222の横には暗証入力装置223とICカード読み取り装置224が設置されている。さらに、それらの機器を制御する入退室管理システム225が背後になり、その中には利用者IDであるパスワード等を登録したデータベース229が存在する。

【0047】ICカード211内には、カード所有者の

アイリストバーン情報220が内蔵されており、ICカード211内の中生体識別照合処理部215bでアイリストバーン処理を行なう際にカード内で利用する仕組みになっている。パスワードが分かっていてもICカード211内のアイリストバーン情報220そのものはICカード211の外部から読み込むことが不可能な仕組みになっている。つまり、ICカード211の外部よりアイリストバーン情報220またはアイリストバーン情報+パスワード情報をICカード211に送信して認証結果(認証率)の情報を返してもらうよう構成されている。

【0048】各種データを読む際にもアイリストバーン情報またはアイリストバーン情報+パスワードが一致しない限り読みない。この構成が第1実施例と大きく異なる点である。

【0049】図6は本発明の第2実施例のICカードを用いた本人確認のフローチャートである。この図を参照しながら、入退室管理システムにおいて、どのようにして本人認証を行なうのか、その動作を説明する。

【0050】(1)まず、入退室管理システム225側では、入室しようとしている人がドア222の前に立ちICカード211を入力すると、カメラ221は立っている人のアイリストバーン情報220を読み込む(ステップS21)。

【0051】(2)次に、読み込んだアイリストバーン情報220(アイリストバーン+パスワードでも可)をICカードに送信する(ステップS22)。

【0052】(3)次に、ICカード内処理を行う。つまり、ICカード側では、外部の装置からアイリストバーン情報を受け取る(ステップS23)と、ICカード内のアイリストバーン情報と比較照合し(ステップS24)、照合率が設定値以上ならICカード内部の利用者IDを読み取り(ステップS25)、アイリストバーン情報照合結果(照合率)と利用者IDを回答する(ステップS26)。

【0053】(4)次に、入退室管理システム225側では、ICカード内照合結果と利用者IDを受け取る(ステップS27)。

【0054】(5)次に、受け取った照合率とその部屋のセキュリティレベルにより、受け取った予め定めた条件に従って照合結果(OK/NG)を判定する(ステップS28)。

40

【0055】(6) 次に、利用者IDを検索する(ステップS29)。

【0056】(7) 次に、利用者IDをチェックする(ステップS30)。

【0057】(8) 登録されている利用者だったら、ドアを開く(ステップS31)。

【0058】また、ステップS28及びステップS30においてNGの場合には終了する。

【0059】なお、ステップS22において、アイリス情報だけでなく、パスワードにより認証を付加するようにしてもよい。

【0060】上記したように、本発明の第2実施例によれば、

(A) 入退室管理システム側のデータベースに利用者のアイリスピターン情報を登録しておく必要がないため、アイリスピターン情報が漏洩・改ざんされることがない。

【0061】(B) 利用者は自分のアイリスピターン情報を登録しているICカードを自分自身で持ち歩けることから安心して利用できる。

【0062】(C) ICカードを紛失した場合でも、ICカード内のアイリスピターン情報を書き換えないため、他人が自分になりますして、入室するという心配がない。さらに、アイリスピターン情報をなくしてカード内の一情報は読み取ることができないため、個人情報が他人に読まれる心配もない。(注:統計で3回照合率が設定値以下ならICカード自身がカードを無効化するなどの仕組みが可能である。)

(D) アイリスピターン情報はICカード内に格納されておりオンラインでやりとりする必要がないため、広域に点在するドアなど、オンライン化が困難な場合であっても、各所にアイリスピターンデータのデータベースを置く必要がなく対応可能である。コスト面・保守面でも有利である。

【0063】(E) アイリスによる照合・パスワード+アイリスによる2重の照合など、照合の方法はICカードを利用するシステムによって自由に決められる。判定結果は照合率(%)で得られるため、入退室のセキュリティレベル(セキュリティ必要度)に応じて照合率の下限を選択可能である。

【0064】(F) オンライン化の必要性がないため、ICカードは異なるシステム間で共通に利用しやすい。

【0065】(G) パスワードは本人の記憶によるため忘れてしまう場合がある。人によっては忘れないように手元にパスワードのメモを残しておき、そのメモからパスワードを盗まれるケースがある。その点アイリスを用いた認証では本人がパスワードを記憶していくても可能なため、忘れてしまったり、メモ等から盗まれるといつた心配がない。

【0066】次に、本発明の第3実施例について説明す

10

る。

【0067】図7は本発明の第3実施例を示すICカードを利用した本人認証手段の模式図、図8は生体識別情報内のデータ構成例を示す図である。

【0068】この図において、311はICカード、312はICカード内に内蔵されるICチップ、313はパスワード又は生体識別情報、314は照合結果+過去3回の照合履歴情報、315はICチップ内のアクセスコントロール部、315aはそのアクセスコントロール部のパスワード情報照合処理部、315bは生体識別照合処理部、316aはパスワード情報記憶部、316bは生体識別情報(ここでは、アイリスピターン)記憶部、317は各種情報記憶部である。

【0069】また、図8に示すように、生体識別情報記憶部316b内にはアイリスピターンデータ316b1、過去3回(最新3回)の照合履歴316b2のデータを有している。

【0070】このように、この実施例は、第2実施例とほぼ同様であるが、ここではアイリスピターンのような生体識別情報内に照合履歴も保管するように構成した点が異なっている。

【0071】なお、第1実施例、第2実施例に共通するが、生体識別照合の場合は一般的に100%の照合が困難である。現実的には何%以上ならOKといった具合にしきい値を設けるものである。

【0072】また、照合率は個人差があり、身体の経年変化などもある。

【0073】この第3実施例では、照合履歴(例えば過去3回分の照合率)をICカード内に持つことで、照合率の個人差や経年変化による影響を改善するようにしている。

【0074】図9は図7及び図8に示した生体識別内蔵ICカードによる本人認証を入退室管理システムに応用した例を説明するための模式図、図10は第3実施例の入退室管理システムの動作フローチャートである。

【0075】(1)まず、入室しようとしている人がドア322の前に立ちICカード311を暗唱入力装置323へ挿入すると、カメラ321は立っている人のアイリスピターンを読み込む(ステップS41)。

【0076】(2)次に、読み込んだアイリスピターン情報(アイリスピターン+パスワード情報でも可)をICカード311へ送信する(ステップS42)。

【0077】(3)次に、ICカード311側では、外部の装置からアイリスピターン情報を受け取る(ステップS43)。

【0078】(4)次に、ICカード311内のアイリスピターン情報と比較照合する(ステップS44)。

【0079】(5)次に、照合率が設定値以上ならICカード内部の過去3回分の照合履歴(最新3回)と利用者IDを読み取る(ステップS45)。

40

【0080】(6) 次に、過去3回の照合履歴を、今回を含めた最新3回分に更新する(ステップS46)。

【0081】(7) 次に、今回の照合結果(照合率)、過去3回分の照合履歴(照合率)、利用者IDを回答する(ステップS47)。

【0082】(8) 次に、入退室管理システム側では、それらを受け取り(ステップS48)、その今回照合率、過去3回分の照合率により、予め定めた条件に従つて照合結果(OK/NG)を判定する(ステップS49)。

【0083】(9) 次に、結果がOKならば利用者IDをデータベースより検索する(ステップS50)。

【0084】(10) 次に、利用者IDをチェックし(ステップS51)。登録されている利用者だったらドアをオープンする(ステップS52)。

【0085】なお、ステップ49及びステップ51においてNGの場合には、処理終了する。

【0086】図11は本発明の第3実施例を示す照合結果OK/NGの判断処理の詳細を示すフローチャートである。

【0087】(1)まず、今回照合率が設定値以上か否かを判定する(ステップS61)。設定値以下で、かつ過去3回も設定値以下か否かを判断し(ステップS65)、以下であれば、ICカードの無効化処理を行い(ステップS66)、結果をNGとする(ステップS67)。

【0088】上記ステップS61において、設定値以上ならば、過去3回分の照合率から平均照合率(個人差あり)を計算する(ステップS62)。さらに、この平均照合率と今回照合率とを比較し(ステップS63)、今回照合率が、過去3回の平均照合率-10%以上の数値であれば結果をOKとする(ステップS64)。そうでなければ、結果をNG(ステップS67)。

【0089】図12は本発明の第3実施例を示す結果判定例を示す図である。

【0090】この図では、具体的な3種類のケースを示している。ケース1では、今回照合率が70%と低かったが、過去3回の平均照合率も低いため結果はOKとなっている。

【0091】一方、ケース2では、ケース1より今回照合率が高いにもかかわらず、過去3回分の平均照合率が良かったため結果がNGとなっている。ケース3は、過去3回及び今回の照合率が設定値以下だったためICカードを無効とした例である。

【0092】この判定方法の例は、比較的簡単な計算手法を用いたが、その他に過去3回分の変化(傾き)やばらつき具合を含めて計算するなど考えられる。

【0093】本発明では過去の照合率をもとに今回照合の判定をしている点が特徴であり、計算手法によらな

【0094】このように、毎回履歴を更新していくことにより、個人差(アイリスパターンの読みやすさなど)や、経年変化(老齢化によるアイリスパターンの変化など)に対応可能となる。

【0095】以上、実施例で示した生体識別方法は、アイリス(瞳の模様)を利用した例であったが、他の生体識別手法においてもそのまま適用可能である。他の生体識別手法とは、例えば、DNA分析、性別判断、病気の遺伝的素因、血液型などの固有の遺伝的特徴を用いたものの、指紋、歯形、掌紋、足型、顔立ち、耳形、網膜血管パターン、手や手首の血管パターン、音声、頬血管パターンなどの固有の外観的特徴を用いたものがある。

【0096】また、ICカードにおいては、カード型のものにかかわらず、腕時計埋め込み型、指輪型、身体埋め込みチップなど、プログラム内蔵型のICメモリを利用したものであれば適用可能である。

【0097】上記した実施例では生体識別内蔵ICカードを利用した入退室管理について説明したが、他に建物の防犯、貸し金庫、銀行窓口、クレジットカード取り引き、電子商取引き、コンピュータや重要なデータベースへのアクセス制御、バスポート、免許証カード、健康保険証カード、自治体窓口での証明書発行・申請、選挙投票、飛行機等乗り物への搭乗手続き、賃貸登録など、高度な本人認証を必要とする広い分野へ適用可能である。

【0098】また、本発明は上記実施例に限定されるものではなく、本発明の趣旨に基づいて種々の変形が可能であり、これらを本発明の範囲から排除するものではなくい。

#### 【0099】

【発明の効果】以上、詳細に説明したように、本発明によれば、以下のようないくつかの効果を奏すことができる。

#### 【0100】(A)

(1) 入退室管理システム側のデータベースに利用者のアイリスパターン情報を登録しておく必要がないため、アイリスパターンの漏洩やそれを改ざんされることがなくなる。

【0101】(2) 利用者は自分のアイリスパターン情報が登録されているICカードを自分自身で持ち歩けることから安心して利用できる。

【0102】(3) ICカードを紛失した場合でも、ICカード内のアイリスパターン情報を書き換えられないため、他人が自分になりますしてそのICカードを利用して入室するという心配がない。

【0103】(4) アイリスパターンはICカード内に格納されており、オンラインでやり取りする必要がないため、広域に点在するドアなど、オンライン化が困難な場合であっても、各所にアイリスパターンデータのデータベースを置く必要がなく対応可能である。コスト面・保守面でも有利である。

【0104】(5) パスワードによる照合、アイリスに

よる照合、パスワード+アイリスによる2重の照合など、照合の方法はICカードを利用するシステムによって自由に決められるため、入退室のセキュリティレベル（セキュリティ必要度）に応じて選択可能である。但し、パスワードが盗まれればICカード内の各種情報が読まれてしまうという危険はある。（注：パスワード 자체はICカードから読めない仕組みであり、続ける3回パスワードを間違えるとICカード自身がカードを無効化するなどの仕組みはついている。）（6）オンライン化の必要性がないため、ICカードは異なるシステム間で共通に利用しやすい。

#### 【0105】〔B〕

（1）個人差（目の開き具合、色の違い等）によるアイリスピターンの読み取りやすさの違いにより、照合判定基準を変えられる（個人差を吸収できる）。

【0106】（2）利用者のアイリスピターンの高齢化や環境変化による経年変化とともに、判定基準が低下していくため、柔軟に追従できる。追従できなくなったらそこでICカードは自動的に無効となる（経年変化を吸収できる）。等の効果がある。

#### 【図面の簡単な説明】

【図1】本発明の第1実施例を示すICカードを利用した本人認証手段の模式図である。

【図2】本発明の第1実施例を示す生体識別内蔵ICカードによる本人認証方法を入退室管理システムに応用した例の模式図である。

【図3】本発明の第1実施例を示すICカードを利用した本人認証動作フローチャートである。

【図4】本発明の第2実施例を示すICカードを利用した本人認証手段の模式図である。

【図5】本発明の第2実施例を示す生体識別内蔵ICカードによる本人認証方法を入退室管理システムに応用した例の模式図である。

【図6】本発明の第2実施例のICカードを用いた本人確認動作フローチャートである。

【図7】本発明の第3実施例を示すICカードを利用した本人認証手段の模式図である。

【図8】本発明の第3実施例を示すICカードの生体識別情報内のデータ構成例を示す図である。

【図9】図7及び図8に示した生体識別内蔵ICカードによる本人認証方法を入退室管理システムに応用した例の模式図である。

\* 【図10】本発明の第3実施例を示す入退室管理システムの動作フローチャートである。

【図11】本発明の第3実施例を示す照合結果OK/N

Gの判断処理の詳細を示すフローチャートである。

【図12】本発明の第3実施例を示す結果判定例を示す図である。

【図13】従来のICカードを利用した本人認証手段の模式図である。

【図14】従来型の入退室管理システムにおける本人認証手段の模式図である。

#### 【符号の説明】

111, 211, 311 ICカード

112, 212, 312 ICチップ

113 パスワード情報

114 パスワード情報及び生体識別情報（本人認証）の結果の情報

115, 215, 315 ICチップ内のアクセセントロール部

115a アクセスコントロール部のパスワード及び

#### 20 生体識別情報照合処理部

116a, 216a パスワード情報記憶部

116b, 216b, 316b 生体識別情報記憶部

117, 218, 317 各種情報記憶部

120 アイリス

121, 221 アイリスピターン認識用カメラ

122, 222 入退室する部屋のドア

123, 223 暗証入力装置

124, 224 ICカード読み取り装置

125, 225 入退室管理システム

#### 30 126 アイリスピターン

129, 229 データベース

213 生体識別情報（+パスワード）

214 結果（照合率）情報

215a パスワード照合処理部

215b 生体識別照合処理部

220 アイリスピターン情報

313 パスワード又は生体識別情報

314 照合結果+過去3回の照合履歴情報

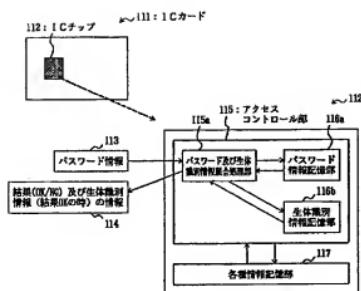
315a アクセスコントロール部のパスワード情報

照合処理部

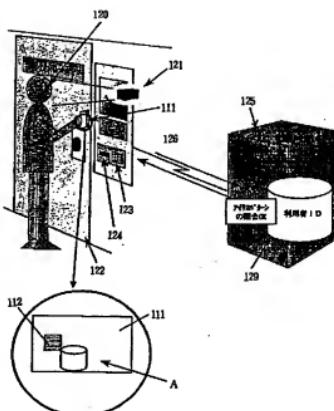
316b1 アイリスピターンデータ

316b2 過去3回（最新3回）の照合履歴

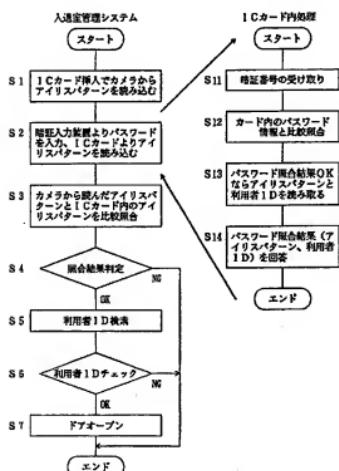
【図1】



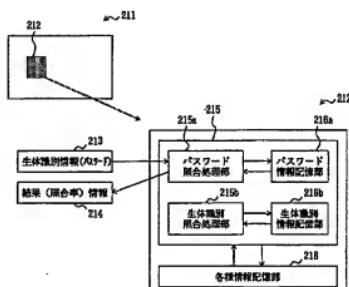
【図2】



【図3】

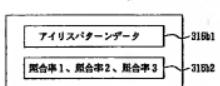


【図4】



【図8】

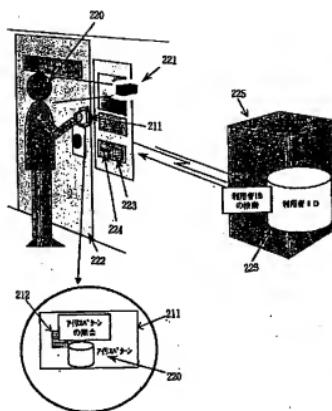
μ～315b: 生体識別情報記憶部 (最低照合率の設定値は50.0%とする)



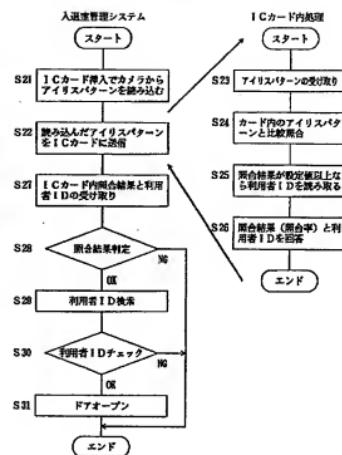
【図12】

ケース	過去5回(実測の1回分)の照合結果	過去3回の平均照合率	今回照合率	判定
1	75.0 % 88.0 % 70.0 %	75.0 %	70.0 %	OK
2	30.0 % 85.0 % 90.0 %	87.5 %	75.0 %	NG
3	60.0 % 50.0 % 60.0 %	56.7 %	50.0 %	NG

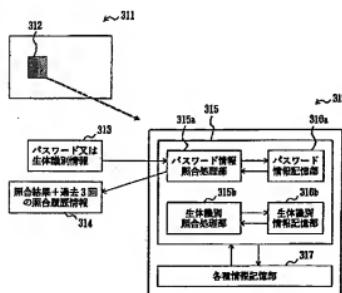
【図5】



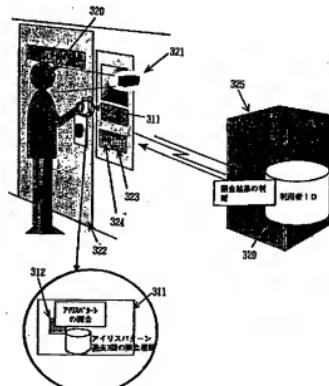
【図6】



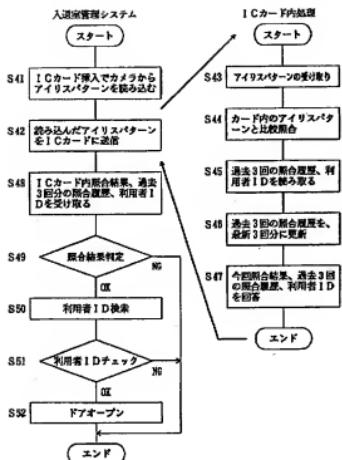
【図7】



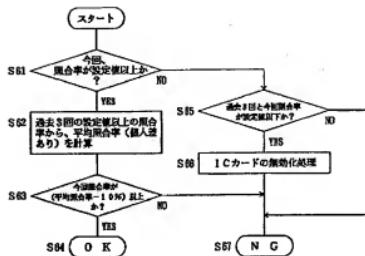
【図9】



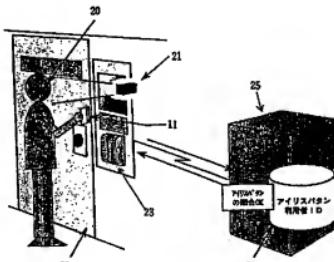
【図10】



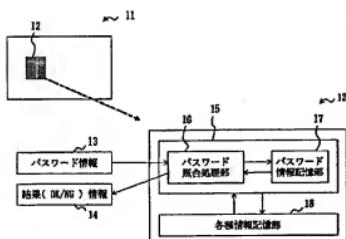
【図11】



【図14】



【図13】



フロントページの続き

Fターム(参考) SB035 AA03 AA14 BC00 BC03 CA22  
 CA38  
 SB043 AA09 BA04 CA10 FA04 FA10  
 GA01 GA19